Research on Information Security Management Strategies in the Digital Transformation of Application-Oriented Universities

Na Ta, Tao Jin*
Ordos Institute of Technology, Ordos 017000, China
Corresponding Author: Tao Jin

Abstract: Against the backdrop of the rapid iteration of digital technologies, the digital transformation of application-oriented universities has become an inevitable trend. This transformation has not only improved the efficiency of campus operations and the quality of services for teachers and students, but also posed new challenges to information security management. This paper explores the significance of digital transformation for information security management in application-oriented universities, and conducts an in-depth analysis of the core risks encountered during the transformation process, including insider operation risks, application system security vulnerabilities, third-party collaboration data leakage risks, mobile terminal usage risks, and AI-related security risks arising from the introduction of artificial intelligence. In response to these risks, this paper proposes targeted implementation strategies: strengthening the overall security protection capabilities through hierarchical and classified security training; preventing system vulnerabilities by means of full-lifecycle system management and deployment of core protective technologies; avoiding data leakage risks relying on the whole-process control of third-party collaborations; blocking the transmission of potential hazards through integrated terminal and network management; addressing AI security risks from multiple dimensions such as data security, algorithm governance, and system integration protection; and building a multi-dimensional information security defense line for the digital transformation of universities.

Keywords: Digitalization of Application-Oriented Universities; Information Security; Management Strategies; Artificial Intelligence

1. Introduction

Application-oriented universities take cultivating practical and skilled talents as their core goal. Their digital transformation covers multiple dimensions, such as the onlineization of teaching resources, the intellectualization of training platforms, the informatization of management services, and the networking of scientific research collaboration. Moreover, the in-depth integration of artificial intelligence technology has become a key support for the transformation. Digital transformation has significantly improved teaching efficiency and optimized the service experience for teachers and students. However, due to the expanded scale of data flow, the complexity of system application scenarios, the broadened boundaries of network access, coupled with additional risks brought by AI technology—such as unfair training evaluation caused by algorithmic bias, difficulties in decision traceability arising from model "black boxes", leakage of sensitive teaching and research information

due to AI training data breaches, and adversarial attacks interfering with the operation of intelligent training systems—it has further given rise to a series of information security risks, including the leakage of teaching data, attacks on training systems, and violations of teachers' and students' privacy.

ARINA [1] in his study pointed out that after the COVID-19 pandemic, when universities extensively adopted tools such as online learning platforms and video conferences for remote teaching, cyber security threats increased significantly. It clearly identifies malware, distributed denial of service (DDoS), and phishing attacks as the three major cyber threats facing universities. A questionnaire survey found that college students have obvious deficiencies in cybersecurity awareness and a lack of understanding of their country's cybersecurity legal framework[2-4].Other studies have found that various factors such as gender and age have no impact on students' cybersecurity awareness, while knowledge reserve is the key factor determining the level of students' cybersecurity awareness[5].Eshetu [6]observed in the study that university websites suffer from vulnerabilities including outdated software and disorganized password management.Therefore, this paper conducts an in-depth study on the information security management issues in the digital transformation of application-oriented universities, identifies potential risks, and proposes targeted strategies. It holds significant practical significance for ensuring the steady progress of the digital transformation of application-oriented universities and safeguarding the safety and stability of education and teaching.

2. The Significance of Digital Transformation for Information Security Management in Application-Oriented Universities

2.1 Ensuring the Continuity of Teaching and Training Activities

Digital teaching resources of application-oriented universities (such as online course videos and virtual simulation experiment data) and training platforms (such as industrial Internet simulation systems and cross-border e-commerce training software) are the core carriers of teaching activities. A sound information security management system can prevent issues like system breakdowns and data loss, ensure the stable conduct of online teaching and remote training, and avoid interruptions to teaching progress caused by security incidents.

2.2 Protecting the Privacy of Teachers and Students and the Security of Sensitive Data

Application-oriented universities have accumulated a large amount of sensitive data in the process of digitalization, including teachers' and students' personal information (such as ID card numbers, contact information, and biometric data), teaching management data (such as academic records and student status information), and practical training and scientific research data (such as cooperative enterprises' business information and technological R&D data). Once this data is leaked or tampered with, it will directly infringe on the privacy of teachers and students, and even cause economic losses to cooperative enterprises, affecting the social credibility of universities. Effective information security management can build a data protection barrier to prevent sensitive information from being illegally obtained or abused.

2.3 Supporting the Secure Implementation of the "Integration of Production and Education" Model

"The integration of production and education" is the core school-running feature of application-oriented universities, and digital transformation provides technical support for in-depth

cooperation between universities and enterprises. Cloud-based training bases co-built by universities and enterprises, as well as shared industry databases, all rely on a secure digital environment. Information security management can address data sharing security issues in university-enterprise cooperation, eliminate enterprises' concerns about the leakage of commercial information, lay a foundation of trust for the long-term advancement of "integration of production and education" projects, and thereby enhance the pertinence and effectiveness of talent cultivation.

3. Analysis of Information Security Management Risks in the Digital Transformation of Application-Oriented Universities

3.1 Insider Operation Risk

Insider operation risk is the most prominent internal security hazard in the digital transformation of application-oriented universities [7-9], which is mainly divided into two categories: unintentional human error risk and intentional operation risk. Among these, unintentional human error risk is the most frequently occurring type of cybersecurity incident in universities currently. The core cause lies in the weak cybersecurity awareness of teachers and students, as well as their lack of relevant knowledge and skills in standardized operations, which easily leads to various potential security hazards. The most common issue is setting simple and easily crackable login passwords. Such passwords are often linked to the campus unified identity authentication system, and once leaked, they may result in illegal intrusions into the internal network. When handling sensitive personal information such as ID card numbers and contact details, some teachers and students also lack information protection awareness and relevant knowledge reserves. They not only fail to adopt security measures such as encrypted storage and desensitized transmission but also may arbitrarily upload and share such information on non-regular platforms. This leads to the illegal scraping and dissemination of teachers' and students' sensitive personal information, resulting in a leakage chaos where "it can be seen everywhere online," seriously infringing on their privacy rights and interests. In addition, if teachers and students accidentally click on phishing links from unknown sources, their terminal devices may be infected with malware, becoming a breakthrough for cyberattacks. These behaviors can directly trigger security incidents such as data leakage and system intrusion, posing a serious threat to campus information security. The other type is intentional operation risk. A small number of personnel will exploit the system access permissions or data access convenience granted by their positions to engage in various malicious acts: stealing sensitive information such as scientific research achievements and students' privacy to seek personal gain through illegal means. Or they may deliberately sabotage core systems such as digital teaching and academic administration management due to personal demands, causing system breakdowns, directly leading to disruptions in core campus businesses, and seriously affecting the progress of university digital transformation and normal school-running order.

3.2 Security Vulnerabilities of Application Systems

In the process of digital transformation, the dependence of application-oriented universities on various digital systems such as teaching platforms, academic administration management systems, and scientific research data centers has risen sharply. Technical flaws are the core source of potential campus information security hazards [10]. First, the digital systems put into use themselves have design flaws, or leave unpatched security vulnerabilities due to inadequate maintenance. These weak points are easily exploited by hackers to carry out malicious activities such as cyberattacks and data

theft. Second, the professional capabilities of technical R&D and operation and maintenance teams are limited, failing to iteratively upgrade outdated systems in a timely manner. This results in incompatibility with new application scenarios such as online teaching and smart management, and the security protection capabilities struggle to meet the needs of digital transformation, forming long-term potential risks. In addition, the lack of sound core protection technology support and the failure to deploy key facilities such as efficient firewalls, data encryption, and intrusion detection and prevention make it difficult to effectively resist security threats like external malicious attacks and network virus intrusions, further amplifying the security risks at the system's technical level.

3.3 Risk of Data Leakage from Third-Party Cooperation

The risk of data leakage from third-party cooperation is a significant external security hazard in the digital transformation of application-oriented universities. These universities often conduct in-depth cooperation with third-party institutions such as technical service providers, cooperative enterprises, and scientific research collaboration units, involving various data circulation scenarios including teaching resource sharing, management system operation and maintenance, and scientific research project collaboration, which makes potential risks increasingly prominent [11]. First, the information security management systems of third-party institutions are inadequate, lacking mature protection technologies and standardized management processes, with uneven protection capabilities. If universities fail to conduct strict review and evaluation of their security qualifications and protection levels before cooperation and blindly share sensitive content such as students' personal information and confidential scientific research data, data leakage is likely to occur due to issues such as attacks on the cooperative partner's systems or internal management irregularities. Second, in university-enterprise cooperation projects, both parties lack clear and detailed agreements on the scope of data sharing, usage scenarios, retention periods, and the division of security responsibilities. Once a data leakage incident occurs, it is prone to ambiguous liability definition and mutual buck-passing, affecting the efficiency of risk disposal. Third, during the internal circulation of data within third-party institutions and among multiple parties, universities find it difficult to implement real-time supervision throughout the entire process and all links. Cooperative partners may use data in violation of agreements beyond the agreed scope, or there may be risks of secondary data circulation and illegal utilization, further exacerbating data security threats.

3.4 Risk of Mobile Terminal Usage

Mobile terminals, including mobile phones, tablet computers, and laptops, are the core carriers for teachers and students to access campus systems and handle official affairs. On one hand, teachers and students often use their personal mobile devices to handle both official and private matters. Some devices lack security protections such as complex passwords and fingerprint recognition, or fail to update systems and install legitimate security software in a timely manner, making them vulnerable to malware implantation and data theft. If a device is accidentally lost or stolen, sensitive content stored on it—such as student information, course materials, and scientific research data—may be directly leaked [12]. On the other hand, to save trouble, some teachers and students use uncertified third-party applications for official tasks or arbitrarily connect to unknown devices for data transmission, which further increases the risks of terminal hijacking and data tampering. Especially for application-oriented universities, teachers and students frequently access scenarios containing sensitive data (such as training management systems and university-enterprise cooperation project

platforms) via mobile terminals, and terminal security vulnerabilities may directly spread to core business systems.

3.5 Security Risks Brought by the Introduction of AI

In the process of digital transformation, the information security management risks brought by AI are mainly reflected in three dimensions: In terms of data security, the massive data relied on by AI training and operation—such as students' personal information and teaching-research data—is prone to leakage, tampering, and unauthorized use during annotation and multi-source fusion, with prominent risks of data ownership disputes [13]; In terms of algorithm security, the "black box" nature of AI leads to opaque decision-making logic, which may trigger discriminatory outcomes. At the same time, AI is vulnerable to adversarial attacks, and biases in training data can cause models to output incorrect conclusions, resulting in obvious vulnerabilities and bias risks [14]; In terms of system and business security, interface compatibility vulnerabilities are likely to occur when AI systems are integrated with universities' existing academic administration, scientific research and other systems. Automated businesses may be maliciously exploited to evade supervision, and improper permission management during operation and maintenance may lead to unauthorized manipulation of models or parameter tampering, undermining system stability [15, 16].

4. Implementation Strategies for Information Security Management in the Digital Transformation of Application-Oriented Universities

4.1 Implementation Strategies for Addressing Insider Operation Risks

A hierarchical and classified security training model should be adopted. First, on-campus personnel are divided into groups based on dimensions such as teaching staff, administrative staff, students, and third-party personnel. Then, differentiated training content is customized according to the work scenarios and risk exposure characteristics of different groups, with core explanations of basic security knowledge including password setting specifications, sensitive data transmission requirements, and phishing link identification skills. Meanwhile, special training is conducted for personnel in key positions such as data administrators and system operation and maintenance staff to clarify their data access boundaries and operational responsibilities, and enhance their risk prevention capabilities in professional fields. During the training, diverse forms such as case teaching, practical exercises, and online quizzes are integrated to promote regular security training. Synchronously, security alert notifications are pushed regularly to comprehensively strengthen the information security awareness of all staff.

4.2 Implementation Strategies for Addressing Security Vulnerabilities of Application Systems

To address the technical security vulnerabilities of digital systems in application-oriented universities, a full-lifecycle security management mechanism for digital systems should be established. In the system selection and design phase, a security assessment process should be introduced, prioritizing the adoption of safe and compliant products suitable for teaching and research scenarios. Meanwhile, regular system security vulnerability scans and penetration tests should be conducted to promptly fix design flaws and unresolved vulnerabilities. Strengthen the professional capacity building of technical R&D and operation and maintenance teams. Improve personnel's security protection skills through special training and external technical cooperation, and steadily promote the iterative upgrading of outdated systems in line with the needs of digital

transformation to ensure system compatibility with new application scenarios. Accelerate the deployment and optimization of core protection technologies. Build a multi-layered security protection system covering efficient firewalls, high-strength data encryption, and intelligent intrusion detection and prevention systems. Combine real-time monitoring and emergency response mechanisms to fully resist security threats such as external malicious attacks and network virus intrusions, thereby reducing campus information security risks at the source.

4.3 Implementation Strategies for Addressing the Risk of Data Leakage from Third-Party Cooperation

To address the risk of data leakage from third-party cooperation, universities should establish a full-process security control mechanism for third-party cooperation. Before cooperation, clear security qualification review standards should be formulated, and strict evaluations should be conducted from dimensions such as the completeness of the information security management system, the maturity of protection technologies, and past security records. Sensitive data-related cooperation should only be carried out with compliant and qualified institutions. Detailed clauses on the scope of data sharing, usage scenarios, retention periods, and the division of security responsibilities should be included in cooperation agreements. The accountability mechanism and compensation standards for leakage incidents should be clarified to avoid ambiguous liability definition. Build a full-process supervision system for data circulation. Adopt technical means such as data desensitization, hierarchical access permissions, and operation log retention to conduct real-time monitoring of data usage, transmission, storage and other links during cooperation. Third parties are prohibited from using data beyond the agreed scope or conducting secondary data circulation. Meanwhile, establish a regular security audit and emergency linkage mechanism. Once irregularities or leakage risks are detected, promptly take measures such as suspending cooperation, data recovery, and risk disposal to fully prevent data security risks arising from third-party cooperation.

4.4 Implementation Strategies for Addressing the Risk of Mobile Terminal Usage

To address the security hazards caused by the risk of mobile terminal usage on campus, the implementation strategy is to establish an integrated management and control mechanism for campus mobile terminals and network security. Clarify the specifications for teachers and students' terminal usage, requiring devices to set complex passwords and enable biometric authentication protection, compelling regular updates of systems and genuine security software, promoting separate storage of official and private data, and encrypting sensitive information. Optimize the campus network security architecture, strengthen wireless network authentication management, and prohibit access to unknown devices and unsafe networks. Meanwhile, build a campus-certified application ecosystem, strictly forbidding the use of uncertified third-party applications for official affairs. Add additional protections such as two-factor authentication and hierarchical permissions for access to sensitive scenarios such as training management systems and university-enterprise cooperation project platforms. Carry out regular security awareness training and practical exercises to improve teachers' and students' capabilities in device loss prevention, malicious program identification, and compliant data transmission. Build a terminal security management platform to realize functions such as device access review, operation log tracing, abnormal behavior early warning, and remote locking/wiping of lost devices, thereby blocking the transmission of terminal security vulnerabilities to core business systems.

4.5 Implementation Strategies for Addressing the Security Risks Brought by the Introduction of AI

To address the security risks brought by the introduction of AI, a full-process data security management and control system can be established. Clarify compliance standards for data collection, annotation, and fusion, and adopt technical means such as encrypted storage and hierarchical permission management to prevent data leakage and unauthorized use. Optimize the algorithm governance mechanism, introduce algorithm auditing and interpretability technologies, reduce model biases through training with diverse datasets, and establish an adversarial attack protection system. In addition, strengthen the integration security testing of AI systems with existing business systems, standardize the supervision process of automated businesses, and improve the AI operation and maintenance permission control and parameter change tracing mechanism to comprehensively resolve security hazards at the data, algorithm, system, and business levels.

4. Conclusion

The digital transformation of application-oriented universities is an inevitable choice to improve the quality of school running and serve regional economic development, and information security management is the "lifeline" to ensure the success of the transformation. Currently, application-oriented universities are facing multi-dimensional risks such as insider operation risks, security vulnerabilities of application systems, the risk of data leakage from third-party cooperation, the risk of mobile terminal usage, and the security risks brought by the introduction of AI. Through strategies such as strengthening compliance management, building a solid technical defense line, optimizing business support, and standardizing data management, application-oriented universities can effectively reduce information security risks and realize the coordinated advancement of digital transformation and security management. In the future, with the in-depth application of technologies such as artificial intelligence and blockchain in the field of education, application-oriented universities need to continuously innovate information security management models—for example, using AI for real-time early warning of security threats and blockchain for data traceability—to continuously improve information security protection capabilities and provide a safe and stable digital environment for cultivating high-quality practical talents.

Acknowledgements

The author thanks the support of the scientific research projects of Inner Mongolia colleges, universities numbered NJZY21153 the science and technology plan project of Ordos City numbered 2021YYI18-46 and Computer Science and Technology Teaching Innovation Team Project of Ordos Institute of Technology, No. 20240403.

References

[1] Arina, A., Network Security Threats to Higher Education Institutions. Central and Eastern European eDem and eGov Days, 2022. 341: p. 323-333.

[2] Bhandari, B., Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks. Unity Journal, 2025. 6(1): p. 120-135.

[3] Chandarman, R. and B.V. Niekerk, Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. The African Journal of Information and Communication, 2017. 20(20): p. 133-155.

[4] Ellala, Z.K., K.M. Al-Tkhayneh, and R.N. Alkhatib, The Extent of Awareness of Cyber Security Among the

Superior and Ordinary Students in the Faculty of Education in Al Ain University. Studies in Systems, Decision and Control, 2023: p. 134-144.

[5] Kamalulail, A., et al., Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. e-Academia Journal, 2022.

[6] Eshetu, A.Y., E.A. Mohammed, and A.O. Salau, Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 2024. 11(1).

[7] Ntloedibe, T., T. Foko, and M.A. Segooa, Cloud leakage in higher education in South Africa: A case of University of Technology. South African Journal of Information Management, 2024. 26(1).

[8] Hills, M. and A. Anjali, A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. Security Journal, 2017. 26(1): p. 275-7.

[9] Robinson, C.N. , and Nikki, The Missing Engineering Discipline in Cybersecurity: Human Factors Engineering. Sage Publications.

[10] Meilong, S., et al., An Approach to Semantic and Structural Features Learning for Software Defect Prediction. Mathematical Problems in Engineering, 2020. 2020.

[11] Gao, H., et al., AI Safety in the Eyes of the Downstream Developer: A First Look at Concerns, Practices, and Challenges. 2025.

[12] Chin, A.G., et al., An Exploration of Mobile Device Security Artifacts At Institutions Of Higher Education. Journal of International Technology and Information Management, 2016.

[13] Guan, X., X. Feng, and A.Y.M.A. Islam, The dilemma and countermeasures of educational data ethics in the age of intelligence. Palgrave Communications, 2023. 9(1): p. 14.

[14] Baker, R. and A. Hawn, Algorithmic Bias in Education. International Journal of Artificial Intelligence in Education, 2021. 32: p. 1052 - 1092.

[15] Sajja, R., et al., Artificial Intelligence-Enabled Intelligent Assistant for Personalized and Adaptive Learning in Higher Education. 2023.

[16] Spring, J.M., et al., On managing vulnerabilities in AI/ML systems. 2021.